

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-374308

(43)Date of publication of application : 26.12.2002

(51)Int.Cl.

H04L 12/66  
G06F 13/00  
G09C 1/00  
H04L 9/14

(21)Application number : 2001-178427

(71)Applicant : MCM JAPAN KK

(22)Date of filing : 13.06.2001

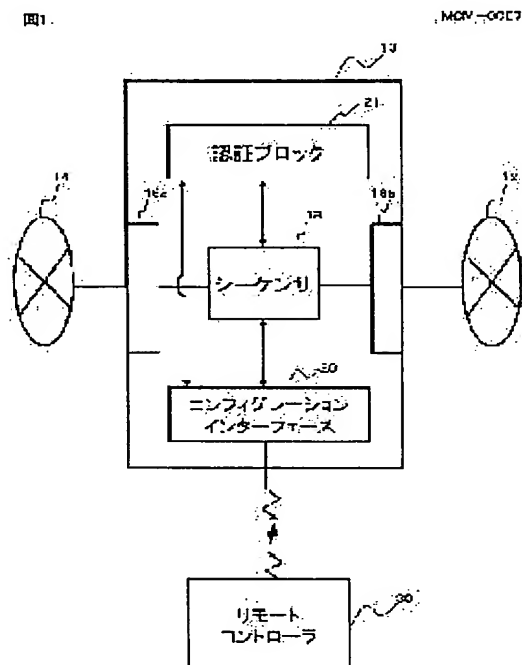
(72)Inventor : SANETO TORU

(54) COMMUNICATIONS EQUIPMENT FOR TRANSMISSION AND CONTROLLING DEVICE FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To realize safety communication, without using authentication servers.

SOLUTION: A configuration interface 20 automatically generates a cryptographic key, based on data communication between with an external remote controller 30. Then, the generated cryptographic key is transmitted to the controller 30 and sent to an authentication block 21. A sequencer 18 decipheres a packet sent from an external network 12, by using the cryptographic key. The sequencer 18 ciphers the packet sent from an internal network 14 by using the cryptographic key. The controller 30, receiving the cryptographic key, stores the cryptographic key in a memory means 36. The cryptographic key inside of the memory means 36 is introduced to another fire wall module via the controller 30. The same cryptographic key can be set easily among a plurality of fire wall modules, to realize cipher communication.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-374308

(P2002-374308A)

(43) 公開日 平成14年12月26日 (2002.12.26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームト* (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 9
G 0 6 F 13/00	3 5 1	C 0 6 F 13/00	3 5 1 Z 5 J 1 0 4
G 0 9 C 1/00	6 6 0	C 0 9 C 1/00	6 6 0 E 5 K 0 3 0
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1

審査請求 未請求 請求項の数19 O L (全 15 頁)

(21) 出願番号 特願2001-178427(P2001-178427)

(22) 出願日 平成13年6月13日 (2001.6.13)

(71) 出願人 595161887

エム・シー・エムジャパン株式会社

東京都世田谷区三軒茶屋2-11-22 サン  
タワーズセンタービル

(72) 発明者 実藤 亨

東京都世田谷区三軒茶屋2丁目11番22号  
サンタワーズセンタービル エム・シー・  
エムジャパン株式会社内

(74) 代理人 100109014

弁理士 伊藤 充

最終頁に続く

(54) 【発明の名称】 伝送用通信機器及びこれを制御する制御機器

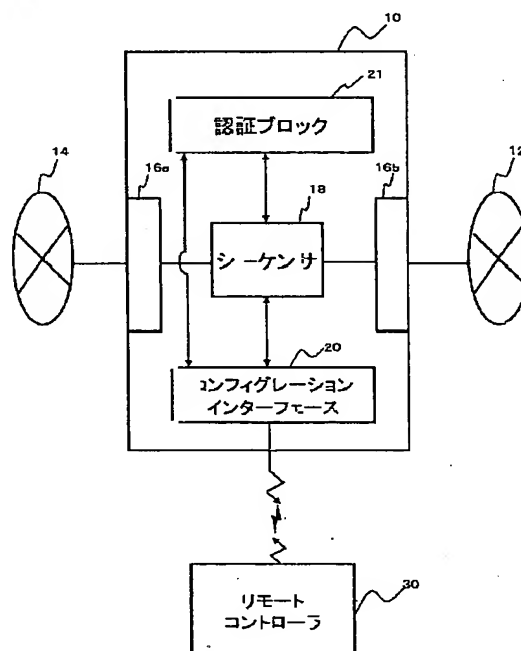
(57) 【要約】

【課題】 認証サーバを用いずに安全な通信を実現する。

【解決手段】 コンフィグレーションインターフェース20は、外部のリモートコントローラ30とのデータ通信に基づき、暗号鍵を自動生成する。そして、生成した暗号鍵は、リモートコントローラ30に送信されると共に、認証ブロック21に送られる。シーケンサ18は、この暗号鍵を用いて外部ネットワーク12から送られてきたパケットを復号化する。シーケンサ18は、この暗号鍵を用いて内部ネットワーク14から送られてきたパケットを暗号化する。暗号鍵を受け取ったリモートコントローラ30はその暗号鍵をメモリ手段36に格納する。そのメモリ手段36内部の暗号鍵をリモートコントローラ30を介して他のファイアウォールモジュール10に導入させる。複数のファイアウォールモジュール10間で容易に同一の暗号鍵を設定することができ、暗号通信を実現できる。

図1

MCM-0007



【特許請求の範囲】

【請求項1】 外部ネットワークと、内部ネットワークとを結ぶ伝送用通信機器において、前記内部ネットワークから送信されたパケットを暗号化してから前記外部ネットワークに送り出し、前記外部ネットワークから送信されてきたパケットを復号化してから前記内部ネットワークに送り出す暗号化復号化手段を含み、前記暗号化復号化手段は、パケット情報と、そのパケット情報に対応した暗号化ビットと、を含むアクセステーブルを備え、前記暗号化復号化手段は、前記内部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを暗号化することを特徴とする伝送用通信機器。

【請求項2】 請求項1記載の伝送用通信機器において、前記暗号化復号化手段は、前記外部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを復号化することを特徴とする伝送用通信機器。

【請求項3】 請求項1又は2記載の伝送用通信機器において、前記パケット情報は、IPフィールドの情報、又は、TCP/UDPフィールドの情報を含むことを特徴とする伝送用通信機器。

【請求項4】 請求項1又は2記載の伝送用通信機器において、前記暗号鍵を生成する暗号鍵管理手段、を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を外部に送信することを特徴とする伝送用通信機器。

【請求項5】 請求項4記載の伝送用通信機器において、前記暗号鍵管理手段は、外部と無線による通信を行い、前記外部からの指示は、前記無線による通信によって受信することを特徴とする伝送用通信機器。

【請求項6】 請求項4記載の伝送用通信機器において、前記暗号鍵管理手段は、外部と赤外線による通信を行い、前記外部からの指示は、前記赤外線による通信によって受信することを特徴とする伝送用通信機器。

【請求項7】 請求項1又は2記載の伝送用通信機器において、前記暗号鍵を生成する暗号鍵管理手段と、

着脱可能な可搬型のメモリ手段にデータを書き込むメモリインターフェースと、を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を前記メモリインターフェースを介して前記メモリ手段に格納することを特徴とする伝送用通信機器。

【請求項8】 伝送用通信機器に対して、指示を出す制御機器において、前記伝送用通信機器と無線による通信を行う通信手段と、利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、を含み、前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器。

【請求項9】 伝送用通信機器に対して、指示を出す制御機器において、前記伝送用通信機器と赤外線による通信を行う通信手段と、利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、を含み、前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器。

【請求項10】 請求項4記載の伝送用通信機器において、前記暗号鍵を格納する暗号鍵格納手段、を有し、前記暗号鍵管理手段は、前記外部から前記暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器。

【請求項11】 請求項7記載の伝送用通信機器において、前記暗号鍵を格納する暗号鍵格納手段、を有し、前記暗号鍵管理手段は、前記メモリインターフェースを介して、前記メモリ手段に格納されている暗号鍵を読み出し、読み出した前記暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器。

【請求項12】 請求項8記載の制御機器において、前記伝送用通信機器と無線による通信を行う通信手段と、利用者の操作に基づき、前記着脱可能な可搬型のメモリ

手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、を含むことを特徴とする制御機器。

【請求項13】 請求項9記載の制御機器において、前記伝送用通信機器と赤外線による通信を行う通信手段と、

利用者の操作に基づき、前記着脱可能な可搬型のメモリ手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、を含むことを特徴とする制御機器。

【請求項14】 コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を前記外部に送信する通信手順と、を実行させることを特徴とするプログラム。

【請求項15】 請求項14記載のプログラムにおいて、前記コンピュータに、外部から暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を、暗号鍵を格納する手段に格納する手順、

を実行させることを特徴とするプログラム。

【請求項16】 コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、

を実行させることを特徴とするプログラム。

【請求項17】 請求項16記載のプログラムにおいて、前記コンピュータに、利用者からの指示に基づき、前記着脱可能なメモリ手段に格納されている暗号鍵を読み出す読み出し手順と、前記読み出した暗号鍵を、暗号鍵を格納する手段に格納する手順、

を実行させることを特徴とするプログラム。

【請求項18】 コンピュータを伝送用通信機器として動作させるプログラムを格納した記録媒体において、前記プログラムは、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を前記外部に送信する通信手順と、を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体。

【請求項19】 コンピュータを伝送用通信機器として動作させるプログラムを格納した記録媒体において、前記プログラムは、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示

に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、

を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、伝送用通信機器に関する。特にファイアーウォール（Fire Wall）機能を実行する伝送用通信機器に関する。

【0002】

【従来の技術】近年、ネットワークを介した通信が広く利用されている。また、公衆ネットワークだけでなく、プライベートなネットワークも広く利用されている。このプライベートなネットワークも公衆ネットワークに接続され、外部との間で通信が行えるのが通例である。

【0003】また、公衆ネットワークを介した通信においては、通信の秘密を守るために、暗号の技術が広く利用されている。この暗号技術の運用の方法は種々知られているが、通信を行う者たち以外の第三者である認証サーバを設ける手法が一般に多く利用されている。

【0004】

【発明が解決しようとする課題】たとえば、一般の家庭内に設けられているような小規模なプライベートネットワークを利用している者にとってわざわざ認証サーバを利用するのは手続きが煩雑になりがちである。

【0005】その一方、外部から、自由にこのプライベートなネットワークにアクセスしたいという要求は多い。たとえば、家庭内のプライベートなネットワーク（以下、内部ネットワークと呼ぶ）の利用者が、出張先から家庭の自分のパーソナルコンピュータのハードディスクの内容を見たい場合等が考えられる。この場合、悪意の第三者のアクセスを防止するために、従来は認証サーバを介した煩雑な手続きを踏む必要があった。

【0006】そのため、認証サーバを使用せずに簡易に安全な通信ができれば便利である。

【0007】また、内部ネットワークが社内ネットワークである場合でも同様の事情が存在する。たとえば、通常はプライベートな社内ネットワーク上（内部ネットワーク上）で仕事をしつつ、出張の際には外部の出先から社内ネットワーク（内部ネットワーク）にアクセスしたいという要望が現実と考えられる。このような要望を、認証サーバを利用せずに実現できれば円滑に業務を遂行でき便利である。

【0008】本発明はこのような課題に鑑みなされたものであり、その目的は、認証サーバを利用せずに、安全な通信をネットワーク上で行うことである。

【0009】

【課題を解決するための手段】本発明は、上記課題を解決するために、外部ネットワークと、内部ネットワーク

とを結ぶ伝送用通信機器において、前記内部ネットワークから送信されたパケットを暗号化してから前記外部ネットワークに送り出し、前記外部ネットワークから送信されてきたパケットを復号化してから前記内部ネットワークに送り出す暗号化復号化手段を含み、前記暗号化復号化手段は、パケット情報と、そのパケット情報に対応した暗号化ビットと、を含むアクセステーブルを備え、前記暗号化復号化手段は、前記内部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを暗号化することを特徴とする伝送用通信機器である。

【0010】このような構成によって、自動的に暗号化を行うことができる伝送用通信機器を実現できる。

【0011】また、本発明は、前記暗号化復号化手段は、前記外部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを復号化することを特徴とする伝送用通信機器である。

【0012】このような構成によって、自動的に暗号化されたパケットを復号化することができる。

【0013】また、本発明は、前記パケット情報は、IPフィールドの情報、又は、TCP/UDPフィールドの情報を含むことを特徴とする伝送用通信機器である。

【0014】このような構成によって、パケットの送信元、宛先を正確に知ることができる。

【0015】また、本発明は、前記暗号鍵を生成する暗号鍵管理手段、を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を外部に送信することを特徴とする伝送用通信機器である。

【0016】このような構成によって、暗号鍵を単に生成させるだけでなく、外部に取り出すことができるので、他の通信機器に暗号鍵を導入することが容易となる。

【0017】また、本発明は、前記暗号鍵管理手段は、外部と無線による通信を行い、前記外部からの指示は、前記無線による通信によって受信することを特徴とする伝送用通信機器である。

【0018】無線による通信を行うので、遠距離から指示を出すことが可能である。

【0019】また、本発明は、前記暗号鍵管理手段は、外部と赤外線による通信を行い、前記外部からの指示は、前記赤外線による通信によって受信することを特徴とする伝送用通信機器である。

【0020】赤外線による通信を行うので、遠距離から指示を出すことが可能である。

【0021】また、本発明は、前記暗号鍵を生成する暗号鍵管理手段と、着脱可能な可搬型のメモリ手段にデータを書き込むメモリインターフェースと、を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を前記メモリインターフェースを介して前記メモリ手段に格納することを特徴とする伝送用通信機器である。

【0022】このような構成によれば、生成した暗号鍵をメモリ手段に自動的に格納することができる。

【0023】また、本発明は、伝送用通信機器に対して、指示を出す制御機器において、前記伝送用通信機器と無線による通信を行う通信手段と、利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、を含み、前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器である。

【0024】このような構成によれば、伝送用通信機器に暗号鍵を生成させると共に、その暗号鍵をメモリ手段に格納することができる。

【0025】また、本発明は、伝送用通信機器に対して、指示を出す制御機器において、前記伝送用通信機器と赤外線による通信を行う通信手段と、利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、を含み、前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器である。

【0026】このような構成によれば、赤外線通信によって伝送用通信機器に暗号鍵を生成させると共に、その暗号鍵を赤外線通信を用いて受け取ってメモリ手段に格納することができる。

【0027】また、本発明は、前記暗号鍵を格納する暗号鍵格納手段、を有し、前記暗号鍵管理手段は、前記外部から前記暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器である。

【0028】このような構成によって、外部からの暗号鍵をその伝送用通信機器に導入させることができる。

【0029】また、本発明は、前記暗号鍵を格納する暗号鍵格納手段、を有し、前記暗号鍵管理手段は、前記メモリインターフェースを介して、前記メモリ手段に格納されている暗号鍵を読み出し、読み出した前記暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器である。

【0030】このような構成によって、メモリ手段に格納されている暗号鍵をその伝送用通信機器に導入させることができる。

【0031】また、本発明は、前記伝送用通信機器と無線による通信を行う通信手段と、利用者の操作に基づき、前記着脱可能な可搬型のメモリ手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、を含むことを特徴とする制御機器である。

【0032】このような構成によって、無線通信を介して暗号鍵を伝送用通信機器に供給することができる。

【0033】また、本発明は、前記伝送用通信機器と赤外線による通信を行う通信手段と、利用者の操作に基づき、前記着脱可能な可搬型のメモリ手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、を含むことを特徴とする制御機器である。

【0034】このような構成によって、赤外線通信を介して暗号鍵を伝送用通信機器に供給することができる。

【0035】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を前記外部に送信する通信手順と、を実行させることを特徴とするプログラムである。

【0036】このようなプログラムを用いれば、暗号鍵を生成する伝送用通信機器を実現することができる。

【0037】また、本発明は、前記コンピュータに、外部から暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を、暗号鍵を格納する手段に格納する手順、を実行させることを特徴とするプログラムである。

【0038】このようなプログラムを用いれば、送信されてきた暗号鍵を内部に格納する伝送用通信機器を実現することができる。

【0039】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、を実行させることを特徴とするプログラムである。

【0040】このようなプログラムを用いれば、暗号鍵を生成すると共にその暗号鍵をメモリ手段に格納する伝送用通信機器を実現することができる。

【0041】また、本発明は、前記コンピュータに、利用者からの指示に基づき、前記着脱可能なメモリ手段に格納されている暗号鍵を読み出す読み出し手順と、前記読み出した暗号鍵を、暗号鍵を格納する手段に格納する手順、を実行させることを特徴とするプログラムである。

【0042】このようなプログラムを用いれば、暗号鍵をメモリ手段から読み取り、内部に格納する伝送用通信機器を実現することができる。

【0043】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムを格納した記録媒体において、前記プログラムは、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を前記外部に送信する通信手順と、を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体である。

【0044】このような記録媒体をコンピュータに組み込むことによって、暗号鍵を生成する伝送用通信機器を構成することができる。

【0045】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムを記録した記録媒体において、前記プログラムは、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体である。

【0046】このような記録媒体をコンピュータに組み込むことによって、暗号鍵を生成すると共にその暗号鍵をメモリ手段に格納する伝送用通信機器を構成することができる。

【0047】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【0048】実施の形態1

図1には、本実施の形態1のファイアーウォールモジュール(Fire Wall Module)10の構成ブロック図が示されている。この図に示すように、ファイアーウォールモジュール10は、インターネット等の外部ネットワーク12と社内ネットワーク等の内部ネットワーク14とを結ぶファイアーウォールモジュール10である。また、ファイアーウォールモジュール10は、この内部ネットワーク14に接続するためのインターフェース16aを備えている。

【0049】さらに、ファイアーウォールモジュール10は、外部ネットワーク12と接続するためのインターフェース16bを有している。そして、ファイアーウォールモジュール10は、外部ネットワーク12と、内部ネットワーク14との間のデータの流れを制御するシーケンサ18を備えている。

【0050】このシーケンサ18は、アクセステーブルを有しており、このアクセステーブルの内容に従って、相手先によってはデータの暗号化や復号化を行う。

【0051】ファイアーウォールモジュール10は、本発明の伝送用通信機器の一例であり、シーケンサは、本発明の暗号化復号化手段の一例である。

【0052】本実施の形態1において特徴的なことは、ファイアーウォールモジュール10が、コンフィグレー

ションインターフェース20を備えていることである。このコンフィグレーションインターフェース20は、外部のリモートコントローラ30とのデータ通信によって、暗号鍵とIDを自動生成する。そして、生成した暗号鍵とIDは、リモートコントローラ30に送信されると共に、認証ブロック21に送られる。さらに、暗号鍵とIDはリモートコントローラ30にも送信される。データ通信は、種々の通信手法を採用することが好ましい。たとえば、赤外線通信や、電波による無線通信を行うことが好ましい。本発明の請求項における「無線」とは、この電波による無線通信を意味する。リモートコントローラ30については後に詳述する。

【0053】コンフィグレーションインターフェース20は、本発明の暗号鍵管理手段の一例である。また、認証ブロック21は、本発明における暗号鍵格納手段の一例である。

【0054】また、上述したように、シーケンサ18は、暗号化／復号化を実行するが、その際に利用する暗号鍵は、認証ブロック21から必要に応じて供給される。

【0055】本実施の形態1において特徴的なことは、ファイアウォールモジュール10が、認証ブロック21を備えていることである。この認証ブロック21は、ファイアウォールモジュール10同士が通信を行う際に、相手側のファイアウォールモジュールの識別動作を主に実行する。

【0056】このような認証ブロック21を備えることによって、ファイアウォールモジュール10同士による安全な通信を実現することができる。この認証ブロック21の動作については後に詳述する。

【0057】リモートコントローラ30の構成ブロック図が図2に示されている。この図に示すように、リモートコントローラ30は、コンフィグレーションインターフェース20との通信手段32と、制御手段34と、メモリ手段36と、を備えている。また、制御手段34にはボタンスイッチ34aとボタンスイッチ34bとが接続している。

【0058】通信手段32は、赤外線通信や無線通信によって、コンフィグレーションインターフェース20との通信を行う手段である。制御手段34はこの通信手段32を用いてコンフィグレーションインターフェース20との間で暗号鍵やIDの生成に必要なデータの送受信、さらにはコンフィグレーションインターフェース20が生成した暗号鍵及びIDの受信、等を行う。

【0059】制御手段34は、利用者がボタンスイッチ34aを押下した場合、通信手段32を介してコンフィグレーションインターフェース20に新たな暗号鍵及びIDの生成を指示する。この指示に基づき、コンフィグレーションインターフェース20は新たな暗号鍵及びIDを生成し、生成した暗号鍵とIDをリモートコントロ

ーラ30に送信してくる。

【0060】また、制御手段34は、通信手段32がコンフィグレーションインターフェース20から生成した暗号鍵とIDとを受信した場合、この暗号鍵及びIDをメモリ手段36に格納する。このメモリ手段36は、リモートコントローラ30から着脱自在に構成されており、リモートコントローラ30以外のパーソナルコンピュータや各種通信装置に接続可能に構成されている。メモリ手段36は、たとえば各種ICカードや各種のフラッシュメモリを用いることが好ましい。もちろん、フレキシブルディスク等の磁気記録手段を利用してもかまわない。

【0061】さらに、制御手段34は、利用者がボタンスイッチ34bを押下した場合、メモリ手段36に格納されている暗号鍵及びIDを読み出し、通信手段32を介してコンフィグレーションインターフェース20にその暗号鍵及びIDを送信する。暗号鍵及びIDを送信されたコンフィグレーションインターフェース20は、その暗号鍵及びIDを認証ブロック21に送信する。認証ブロック21はこの暗号鍵とIDとを内部に格納する。

【0062】このような構成によって、利用者はこのメモリ手段36を外部に持ち出し、他のファイアウォールモジュール10にこのメモリ手段36を介して暗号鍵とIDとを供給することができる。又は、外部から受け取ったメモリ手段36をリモートコントローラ30に取り付け、このメモリ手段36内に格納されている暗号鍵及びIDを、ファイアウォールモジュール10内に送ることができる。

【0063】このようにして、複数のファイアウォールモジュール10に対して共通の暗号鍵とIDとを設定することができる。その結果、利用者は外部の他のファイアウォールモジュール10を用いて外部ネットワーク12から内部ネットワーク14にアクセスし、IDと暗号鍵を用いた安全な通信を実行することが可能である。

【0064】ここで、他のファイアウォールモジュール10は、他の場所にあるプライベートなネットワークとインターネットを結ぶ箇所に設けることができる。この場合は、そのプライベートなネットワーク上の電子機器から上記アクセスを行うことができる。

【0065】また、他のファイアウォールモジュール10は、個別の電子機器の中に設けても良い。電子機器としては、たとえばパーソナルコンピュータや、携帯電話等を利用することができる。この場合は、利用者は、携帯電話等から、いわゆる移動体通信を利用して内部ネットワーク14に対するアクセスを行うことができる。なお、電子機器としては、いわゆるPDA (Personal Digital Assistant) 等の通信装置を利用してもかまわない。

【0066】このファイアウォールモジュール10



は、本発明の「伝送用通信機器」の一例に相当する。

【0067】また、このリモートコントローラ30は、請求項の「制御機器」の一例である。

【0068】次に、本実施の形態1における具体的な動作原理を図3、図4、図6、図7、図8のフローチャートを用いて詳細に説明する。

【0069】まず、ステップS3-1においては、利用者が外部からアクセスするための暗号鍵とIDを生成するために、リモートコントローラ30を利用して、コンフィグレーションインターフェース20に対して、暗号鍵の生成を指示する。

【0070】この指示においては、暗号鍵とIDの生成に必要なデータの送信が、リモートコントローラ30からコンフィグレーションインターフェース20に対して行われる。このデータには、利用者の名称や、乱数、日付・時刻のデータ、等を含めても良い。

【0071】具体的な利用者の指示動作は、リモートコントローラ30のボタンスイッチ34aの押下によって実行される。このボタンスイッチ34aの押下を制御手段34が検知し、暗号鍵とIDの生成を通信手段32を介してコンフィグレーションインターフェース20に対して指示するのである。

【0072】したがって、本実施の形態1によれば、利用者がファイアウォールに関する知識を有していなくても、単にボタンスイッチ34aを押下するだけで暗号鍵とIDを生成させることができる。このファイアウォール等に代表されるネットワーク機器の設定は非常に煩雑なものである。したがって、従来は、出張者が出張先から社内ネットワーク14にアクセスするために新たに暗号鍵を生成しようと思っても、簡単に暗号鍵とIDを生成させることはできなかった。このような状況下でも本実施の形態1によれば、ネットワーク機器に詳しくない者でも暗号鍵とIDを容易に生成させることができるため、利便性の高いネットワークシステムを構築することができる。

【0073】ステップS3-2においては、コンフィグレーションインターフェース20が上記指示に基づいて暗号鍵とIDを生成する。この暗号鍵とIDは具体的にはそれぞれ8バイト程度のデータ列である。暗号鍵は、シーケンサ18におけるデータの暗号化に利用されるデータである。また、IDは利用者の「識別子」であり、通信している者を特定する役割を果たす。ただし、本実施の形態1では、このファイアウォールモジュール10を利用する者はすべて共通のIDを用いる例を説明している。したがって、本実施の形態1におけるIDはグループのID（識別子）とも言える。

【0074】ステップS3-3においては、この暗号鍵とIDとが認証ブロック21に送られる。この送信は暗号鍵とIDとを作成したコンフィグレーションインターフェース20が実行する。認証ブロック21は、送られ

てきた暗号鍵とIDとを内部に保存する。シーケンサ18は、データの暗号化／復号化の際に、認証ブロック21が格納している暗号鍵を利用する。

【0075】ステップS3-4においては、この暗号鍵とIDがリモートコントローラ30にも送られる。リモートコントローラ30においては、通信手段32を介して受信したこの暗号鍵とIDがメモリ手段36に格納される。なお、ステップS3-3とステップS3-4の実行順序は逆でもかまわない。実際には、これらの送信はほとんど同時に実行されよう。この送信も、暗号鍵とIDとを作成したコンフィグレーションインターフェース20が実行する。

【0076】ステップS3-5においては、利用者はリモートコントローラ30からメモリ手段36を取り出し、内部ネットワーク14に直接アクセスできない外部に持ち出す。このような状況は、たとえば他の支店や、出張等の状況が考えられる。そして、このメモリ手段36を他の支店に設置されているファイアウォールモジュール10に付属するリモートコントローラ30に取り付ける。出張等の場合は、このメモリ手段36を出張者が携帯するノート型コンピュータに内蔵されているファイアウォールモジュール10に付属するリモートコントローラ30に取り付ける。

【0077】なお、リモートコントローラ30は、内部ネットワーク14側と、外部ネットワーク側12との間で共用してもかまわない。すなわち、メモリ手段36をリモートコントローラ30から取り外さずに、リモートコントローラ30ごと外部に持ち出し、支店のファイアウォールモジュール10と無線による通信を行わせても良い。また、リモートコントローラ30ごと外部に持ち出し、ノート型パーソナルコンピュータ内部のファイアウォールモジュール10と通信を行わせても良い。

【0078】さらに、ステップS3-5においては、利用者は、メモリ手段36内に格納されている暗号鍵とIDとを他の支店等におけるファイアウォールモジュール10に供給する。この供給は、利用者がリモートコントローラ30を操作することによって実行する。この実行によって、他の支店等に設けられているファイアウォールモジュール10中の認証ブロック21中に、IDと暗号鍵が格納される。

【0079】具体的には、利用者はリモートコントローラのボタンスイッチ34bを押下する。このボタンスイッチ34bの押下を制御手段34が検知し、メモリ手段36内に格納されている暗号鍵とIDとを通信手段32を介してファイアウォールモジュール10内のコンフィグレーションインターフェース20に送信するのである。コンフィグレーションインターフェース20は、暗号鍵とIDとが送信されてくると、これらを認証ブロック21に送る。認証ブロック21は送られてきた暗号鍵とIDとを内部に格納する。

【0080】このようにして複数のファイアーウォールモジュール10に対して同一の暗号鍵とIDを設定することができる。これらのファイアーウォールモジュール10同士の通信においてはこれらの暗号鍵とIDを用いた安全な通信を行うことができる。

【0081】ステップS3-6においては、利用者が外部の支店や、出張先等からファイアーウォールモジュール10を介して内部ネットワーク14にアクセスを行う。このように、本動作例1においては、同一の暗号鍵及びIDが設定されたファイアーウォールモジュール10同士がインターネット等の公衆ネットワークを介して通信を行う例を示す。

【0082】ステップS3-6におけるファイアーウォールモジュールの詳細な動作を図4、図6、図7、図8のフローチャートに基づき説明する。

【0083】図4は、ファイアーウォールモジュール10を介して内部ネットワーク14から外部ネットワーク12に対してデータを送信する場合のファイアーウォールモジュール10の動作を表すフローチャートである。

【0084】また、図6、図7、図8は、外部ネットワーク12から送られてきたデータをファイアーウォールモジュール10を介して内部ネットワーク14側が受信する場合のファイアーウォールモジュール10の動作を表すフローチャートである。

【0085】送信動作（図4）

まず、ステップS4-1において、シーケンサ18は、内部ネットワーク14からパケットを受信する。そして、シーケンサ18は、このパケットの情報を検査し、そのIPヘッダー又はTCPヘッダーの内容がアクセステーブルに登録されているか否かを検査する。前述したように、シーケンサ18はその内部にアクセステーブルを有している。

【0086】アクセステーブルの様子を表す概念図が図5に示されている。この図に示すように、アクセステーブルは、パケット情報と、ディスティネーションポートナンバー（Destination Port Number）と、暗号化ビットとを含むテーブルである。このテーブルへのデータのエン트리動作、及び暗号化ビットの制御動作については順次説明していく。

【0087】さて、ステップS4-1における検査の結果、登録されている場合には、ステップS4-2に処理が移行し、登録されていない場合は、ステップS4-4に処理が移行する。

【0088】ステップS4-2においては、その登録内容を検査し、暗号化ビットが立っているか否かを検査する。暗号化ビットが立っている場合には、ステップS4-3に処理が移行し、立っていない場合には、ステップS4-5に処理が移行する。

【0089】ステップS4-3においては、暗号化鍵でパケットのデータペイロード部を暗号化する。暗号化し

た後、そのパケットをインターフェース16bを介して外部ネットワーク12に送り出す。

【0090】この暗号化に際しては、シーケンサ18は、認証ブロック21から暗号化鍵を受け取り、暗号化に利用する。

【0091】なお、本実施の形態1のファイアーウォールモジュール10は、暗号化鍵を一度に一種類用いる。すなわち、ファイアーウォールモジュール10を利用する人々は、すべて共通の暗号化鍵及びIDを利用するのである。暗号化鍵を更新する必要がある場合には、再びリモートコントローラ30を操作して暗号化鍵及びIDの生成作業を実行する。そして、生成した暗号化鍵及びIDを各ファイアーウォールモジュール10内の認証ブロック21に格納するのである。

【0092】もちろん、利用者のグループごとに別個の暗号化鍵及びIDを設けるように構成しても良い。

【0093】ステップS4-4においては、そのパケットをアクセステーブルに新たに登録する。登録はそのパケットのパケット情報をテーブルに格納することによって実行する。

【0094】パケット情報とは、IPフィールドや、TCP/UDPフィールドの情報を言い、たとえばIPヘッダーやTCPヘッダー等の情報を意味する。少なくともパケット情報にはIPフィールド又はTCP/UDPフィールドの情報が含まれる。

【0095】そして、ディスティネーションポートナンバーも格納する。さらに、テーブル中の各レコードには、暗号化ビットが設けられている。このように、アクセステーブルの各レコードは、パケット情報と、ディスティネーションポートナンバーと、暗号化ビットとから構成される。暗号化ビットの初期値は立っていない状態「0」である。

【0096】ステップS4-5においては、パケットが暗号化されずにそのままインターフェース16bを介して外部ネットワーク12に送り出される。

【0097】受信動作（図6、図7、図8）

まず、ステップS6-1において、シーケンサ18は、外部ネットワーク14からパケットを受信する。すると、シーケンサ21は、認証ブロック21内のアクセステーブルを読み出し、シーケンサ18が受信したパケットのディスティネーションポートナンバーがアクセステーブルに格納されているか否かを検査する。その結果、アクセステーブル中に一致するディスティネーションポートナンバーがあれば、ステップS6-2に処理が移行し、一致するものがなければ、ステップS6-5に処理が移行する。

【0098】ステップS6-2においては、アクセステーブルとの比較が続行される。具体的には、他のパケット情報も一致するか否かを検査される。この結果、一致すれば、ステップS6-3に処理が移行し、一致しない場

合にはステップS6-4に処理が移行する。

【0099】ステップS6-3においては、そのパケットを内部ネットワーク14に向けて送信する。すなわち、内部ネットワーク12へ侵入するのを許可するのである。この際、アクセステーブルの暗号化ビットが立っている場合には、復号化処理を行ってもかまわない。このように暗号化・復号化処理を行うことによって、通信内容を第三者に知られてしまうことを防止することができる。

【0100】ステップS6-4においては、外部から送信されてきたパケットを廃棄すると共に、そのパケットの送信元へ、応答パケットを送信する。この応答パケットの役割については後述する。

【0101】ステップS6-5においては、ディスティネーションポートナンバーがファイアウォールモジュール10用のポートナンバーであるか否か検査される。この検査の結果、一致すれば図7のステップS7-1に処理が移行し、不一致であればステップS6-6に処理が移行する。

【0102】さて、ファイアウォールモジュール10がパケットを生成した場合に、それに特化したポート番号がアサインされるが、そのポート番号を、ファイアウォールモジュール10用のポートナンバーと言う。

【0103】なお、一致したと言うことは、そのパケットはファイアウォールモジュール10宛のパケットであることを意味する。

【0104】ステップS6-6においては、外部から送られてきたパケットが廃棄される。ポート番号に該当するものがなく、エラーが発生していると考えられるからである。

【0105】図7のステップS7-1においては、パケットのデータペイロード部を認証ブロック21に格納されている暗号鍵を用いて復号化する。

【0106】本実施の形態1においては、ファイアウォールモジュール宛のパケットのデータペイロード部には、IDを格納しておく取り決めを行っている。このような取り決めを行うことにより、不正なアクセスを防止することが可能である。

【0107】ステップS7-2では、復号化したIDを、既に登録済みのIDと比較する。比較の結果、一致すればステップS7-3に処理が移行し、一致しなければ図8のステップS8-1に処理が移行する。

【0108】ステップS7-3においては、アクセステーブルのチェックが実行される。具体的にはIPアドレスの一致等を検査するのである。

【0109】ステップS7-4においては、アクセステーブルのチェックの結果、パケットの送信者が既にアクセステーブルに登録されていればステップS7-5に処理が移行し、登録されていない場合には、ステップS7-9に処理が移行する。

【0110】ステップS7-5においては、IDを所定量だけインクリメントする。この量もあらかじめ取り決めておく。このような量をあらかじめ取り決めておくことによって、インクリメント後のIDを受信した通信の相手側が当方を正しい通信相手と認識することが可能である。

【0111】ステップS7-6においては、インクリメント後のIDを暗号化する。暗号化は認証ブロック21に格納されている暗号鍵を利用して実行する。

【0112】ステップS7-7においては、この暗号化したIDをデータペイロード部に含むパケットを、外部ネットワーク12を介して、先にパケットを送信してきた送信元へ送る。これはいわば送信元にアノリッジを返したことになる。

【0113】ステップS7-8においては、アクセステーブル中の、上記送信元の暗号化ビットを立てて、「1」にする。これによって、以降、その送信元との間の通信は暗号化通信によって実行される。

【0114】ステップS7-9においては、外部から送られてきたパケットが廃棄される。

【0115】次に、ステップS8-1においては、受信したパケット中に格納されているIDを所定量だけデクリメントする。この量は上記インクリメントする量と同一である。

【0116】ステップS8-2においては、デクリメント後のIDが自己のIDと一致するか否か検査する。一致する場合には、ステップS8-3に処理が移行し、不一致の場合はステップS8-4に処理が移行する。

【0117】ステップS8-3においては、アクセステーブルにパケット情報を登録する。パケット情報とは、IPフィールドや、TCP/UDPフィールドの情報を言う。少なくとも、これらの情報には、IPフィールド又はTCP/UDPフィールドの情報が含まれる。

【0118】ステップS8-4においては、パケット情報の登録に引き続き、その新たに登録したレコードの暗号化ビットを立てて「1」にする。これによって、以降、その送信元との間の通信は暗号化通信によって実行される。

【0119】ステップS8-5においては、IDが一致しなかったのであるから、別グループのファイアウォールモジュールからの通信が誤ってなされた等のエラーが発生している。したがって、そのパケットは廃棄される。

【0120】応答パケット

次に、応答パケットについて説明する。ファイアウォールモジュール10は、内部ネットワーク14から送信されてきたパケットのみを外部ネットワーク12に送信するだけでなく、自己が自ら構成したパケットを外部ネットワーク12に送信することもある。これが上記ステップS6-4で言及した応答パケットである。

【0121】 応答パケットの説明図が図9に示されている。

【0122】 図9(1)には応答パケットが示されている。ここに示すように、応答パケットは、IPヘッダーと、TCPヘッダーと、IDが暗号化されたデータと、の3種類のブロックを含んでいる。ここで、TCPヘッダーにおいては、ディスティネーションポートナンバーは、ファイアーウォールモジュール10用のポートナンバーである。このファイアーウォールモジュール10用のポートナンバーを用いることによって、ファイアーウォールモジュール10に対するパケットであることを表すことができる。

【0123】 なお、この応答パケットは、認証ブロック21が作成する。認証ブロック21は、外部からパケットが送信されてきた場合にこのような応答パケットを生成し、外部に出力する(上記ステップS6-4)。

【0124】 図9(2)には、応答パケットを受信したファイアーウォールモジュール10がその応答パケットを受領した旨を表す承認パケットの説明図が示されている。この承認パケットは、上記ステップS7-7において送信されるパケットである。この図に示すように、承認パケットは、IPヘッダーと、TCPヘッダーと、所定量インクリメントされたIDが暗号化されたデータと、の3種類のブロックを含んでいる。ここで、TCPヘッダーにおいては、ソースポートナンバーは、ファイアーウォールモジュール10用のポートナンバーである。このファイアーウォールモジュール10用のポートナンバーを用いることによって、ファイアーウォールモジュール10が送信したパケットであることを表すことができる。

【0125】 なお、この承認パケットも、認証ブロック21が作成する。認証ブロック21は、応答パケットを受信した場合にこの承認パケットを送信することによって暗号通信の準備が完了したことを相手側に伝えることができる。

【0126】 以上述べたような動作を本ファイアーウォールモジュール10は実行する。このような動作によって、具体的には以下のような通信モードを実現することができる。

【0127】 通信モード1(ファイアーウォールモジュール同士の通信)

ファイアーウォールモジュール10同士の通信においては、既に述べたように、あらかじめリモートコントローラ30やメモリ手段36によって、共通の暗号鍵及びIDが各ファイアーウォールモジュール10に設定されている。

【0128】 通信モード1の動作を説明するシーケンス図が図10に示されている。

【0129】 まず、一方のファイアーウォールモジュール10aを含む通信システムから、他方のファイアーウ

オールモジュール10bを含む通信システムへパケットが送信される(100)。この送信の際、新しい相手先であればアクセステーブルに登録されることは既に説明した通りである(ステップS4-4)。

【0130】 次に、上述したように、ステップS6-6に従って、他方のファイアーウォールモジュール10bの認証ブロック21は応答パケットを生成し、これを一方のシステムに返送する。これが図中102で示されている。この応答パケットは暗号化されたIDを含んでいる。

【0131】 応答パケットを受信した一方のファイアーウォールモジュール10aは、IDを復号し(ステップS7-1)、アクセステーブルに登録してあるのを確認し(ステップS7-4)、ステップS7-7において承認パケットを他方のファイアーウォールモジュール10に返送する。これは図中104で示されている。さらに、暗号化ビットも立てられる(ステップS7-8)。

【0132】 承認パケットを受信した他方のファイアーウォールモジュール10bは、ステップS8-1でIDをデクリメントした結果元のIDが得られることを確認した後(ステップS8-2)、アクセステーブルにパケット情報を登録し、暗号化ビットを立てる。

【0133】 以上のようにして、両システムがそれぞれアクセステーブルに登録され、パケットは、ファイアーウォールモジュール10を通過する際に自動的に暗号化、復号化される。そのため、暗号通信を容易に実行することができる。

【0134】 通信モード2(ファイアーウォールモジュール10を用いない相手先)

ファイアーウォールモジュール10は、そのシーケンサ18中にアクセステーブルを有しているため、通信相手ファイアーウォールモジュール10を有しない場合でも、通常通りの通信を実行することが可能である。

【0135】 既に述べたように、ファイアーウォールモジュール10を用いて外部にパケットを送信する場合には、新しい相手であれば必ずアクセステーブルに登録がなされる(ステップS4-4)。

【0136】 したがって、一度アクセスした相手先からパケットが送られてきた場合には、必ずアクセステーブル内のパケット情報と合致するはずである(ステップS6-2、S6-3)。したがって、暗号化の対象とはならず、従来の通常の通信を行うことが可能である。

【0137】 以上述べたように、本実施の形態1によれば、ファイアーウォールモジュール10を用いることによって、たとえば家庭内ネットワークに、外部から公衆ネットを介して安全にアクセスすることが可能である。特に、アクセスする権利を有する利用者群に共通のIDを設定しているため、そのIDを用いたアクセス以外を拒否することができ、安全に通信を行うことが可能である。IDが異なることによって、たとえば「他の家庭の

家庭内ネットワーク」に対するアクセスであると判断することができるものである。

【0138】本実施の形態1によれば、内部ネットワーク14に外部ネットワーク12からアクセスするための暗号鍵とIDを自動的に作成し、さらにその暗号鍵とIDがメモリ手段36に格納されるため、そのメモリ手段36を用いて外部ネットワーク12から容易に保護ネットワーク14へアクセスすることが可能となる。

【0139】そして、第三者の内部ネットワーク14への侵入を防止しつつ、内部ネットワーク14へアクセスする正当な権利を持つ者は、外部ネットワーク12から容易に内部ネットワーク14にアクセスすることができる。

【0140】なお、コンフィグレーションインターフェース20は、赤外線通信や無線通信を行う通信装置と、暗号鍵を生成するプログラムとそのプログラムを実行するプロセッサとから構成される。このプログラムは、図3に示す動作の一部を実行し、リモートコントローラ30からの指示によって暗号鍵とIDを生成し、シーケンサ18や、認証ブロック21、リモートコントローラ30に送信する。

【0141】また、コンフィグレーションインターフェース20と、リモートコントローラ30との間の通信はIrDA等の赤外線通信、Blue Tooth等の無線通信、等を利用することができる。なお、IrDAとは、業界内の標準化組織であるInfrared Data Associationが赤外線データ通信の規格として標準化を行った規格である。Blue Toothとは、複数の電気通信会社が制定した無線通信の規格の名称であり、商標でもある。

【0142】また、リモートコントローラ30の制御手段34は、プログラムとそのプログラムを実行するプロセッサとから構成されている。

【0143】このファイアーウォールモジュール10は、本発明の「伝送用通信機器」の一例に相当する。

【0144】このリモートコントローラ30は、請求項の「制御機器」の一例である。

【0145】ファイアーウォールモジュールの構成  
ファイアーウォールモジュール10は、実際にはLSIで構成することが好ましい。特にシーケンサ18は高速性が要求される場合が多いと考えられるため、ハードウェアで実現することが望ましい場合が多い。

【0146】しかし、高速性がそれほど要求されない用途では、ファイアーウォールモジュール10はプログラムと、そのプログラムを実行するプロセッサとから構成しても良い。このプログラムは、これまで述べたフローチャートに示された動作をコンピュータに実行させるプログラムである。これらのプログラムをハードディスク等の記憶手段に格納したコンピュータを用いて上記ファイアーウォールモジュールと同様の機能を実現することができる。このような構成を表す説明図が図11に示さ

れている。

【0147】この図に示すように、コンピュータ120は、内部のハードディスク122にこれまで述べた動作を実現するプログラムを格納している。そして、プロセッサ124がこのプログラムを実行する。内部ネットワーク14とのインターフェース16aや、外部ネットワークとのインターフェース16bそのものはIEEE802.3等のインターフェースであり、ハードウェアで実現することが好ましい。ただし、外部のリモートコントローラ30とのインターフェースはたとえばIrDA等のインターフェース200を利用することが好ましいが、他のブルートゥース(Blue Tooth)等のインターフェースを利用してもかまわない。また、プログラムはハードディスク122に限らず、種々の光ディスク、半導体記憶装置等を利用しても良い。

【0148】なお、インターフェース16a、16bはハードウェアで実現するのが好ましいと述べたが、そのインターフェースの制御部分はプログラムで構成することが好適であろう。コンフィグレーションインターフェース20の無線通信の部分は、上述したようにIrDAやBluetoothのインターフェースであるが、このインターフェース部分に関してもそのハードウェアの制御はプログラムによって実現することが好ましい。これらのプログラムもハードディスク122に格納しておく。また、図1における認証ブロックは、暗号鍵を保管するが、その保管場所はハードディスク102を利用することが好ましい。すなわち、図11の構成の場合は、図1における認証ブロックは、ハードディスク122内のプログラムだけでなく、その内部の記憶領域によって実現されている。また、図1におけるシーケンサ内部のアクセステーブルも同様にハードディスク122内の記憶領域を用いて構成することが好適である。

【0149】実施の形態2

上記実施の形態1では、リモートコントローラ30にメモリ手段36を装着し、リモートコントローラ30を介して暗号鍵やIDをメモリ手段36に格納した。

【0150】しかし、コンフィグレーションインターフェース20から直接メモリ手段36に暗号鍵やIDを書き込んでも良い。また、コンフィグレーションインターフェース20が、メモリ手段36に格納された暗号鍵やIDを直接読みとつても良い。

【0151】このような構成を表す図が図12に示されている。この図に示すように、コンフィグレーションインターフェース20には、メモリインターフェース22が接続されている。このメモリインターフェース22は、メモリ手段36がICカードの場合には、ICカードリーダ/ライタである。また、メモリ手段36がフラッシュメモリの場合には、フラッシュメモリのリーダ/ライタを用いる。要するに、メモリ手段36にデータを読み書きできる手段であればどのようなものでも良い。

【0152】また、近年USBインターフェースプラグの中にフラッシュメモリ等を組み込んだメモリ製品が利用されている。このようなUSBプラグを利用したメモリをメモリ手段36として用いる場合は、メモリインターフェース22として、USBインターフェースを使用することができる。このように構成すれば、メモリ以外に他のUSBインターフェースを有する機器もファイアーウォールモジュール10に接続することができ、汎用性が高まる。

【0153】なお、図12のような構成を採用した場合、利用者は、リモートコントローラ30のボタンを押下する代わりにファイアーウォールモジュール10に接続されているボタンスイッチ24aを押下することによって、暗号鍵及びIDの生成を指示する。この場合、コンフィグレーションインターフェース20のプログラムは、ボタンスイッチ24aが押下された場合に暗号鍵及びIDの生成を開始するような動作を実行する。

【0154】さらに、コンフィグレーションインターフェース20は、生成した暗号鍵及びIDを、認証ブロック21に送信し、メモリ手段36に書き込む。書き込みは、メモリインターフェース22を用いて実行される。

【0155】逆に、メモリ手段36に格納された暗号鍵及びIDを読み取り、認証ブロック21に格納する動作を実行させるには、利用者はボタンスイッチ24bを押下する。利用者がボタン24bを押下すると、コンフィグレーションインターフェース20のプログラムは、この押下に応じて、メモリ手段36から暗号鍵及びIDを読み出し、認証ブロック21に送信する。認証ブロック21はこの暗号鍵とIDとを内部に格納する。なお、メモリ手段36からの読み出しは、メモリインターフェース22を用いて実行される。

【0156】このように本実施の形態1に示された構成を採用した場合でも、これを図11に示されたようなプログラムを用いた構成としても良い。

【0157】

【発明の効果】以上述べたように、本発明によれば、暗号鍵を伝送用通信機器に自動的に生成させることが可能である。さらに、その暗号鍵を外部に取り出すことができるので、他の伝送用通信機器へ同一の暗号鍵を容易に導入させることが可能である。

【0158】また、本発明によれば、無線通信や赤外線通信によって伝送用通信機器に暗号鍵を自動的に生成させることができる。さらに、その暗号鍵を無線通信や赤外線通信を介して受信し、メモリ手段に格納することができる。その結果、メモリ手段を他のシステムに組み込み、他の伝送用通信機器に対して容易に同一の暗号鍵を導入することができる。

【0159】また、本発明によれば、外部からの暗号鍵を容易に伝送用通信機器に導入させることができる。

【図面の簡単な説明】

【図1】本実施の形態のファイアーウォールモジュールの構成ブロック図である。

【図2】リモートコントローラの構成ブロック図である。

【図3】本実施の形態1の動作を説明するフローチャートである。

【図4】本実施の形態1の動作を説明するフローチャートである。

【図5】アクセステーブルの構成を示す説明図である。

【図6】本実施の形態1の動作を説明するフローチャートである。

【図7】本実施の形態1の動作を説明するフローチャートである。

【図8】本実施の形態1の動作を説明するフローチャートである。

【図9】応答パケットと承認パケットの構成を示す説明図である。

【図10】ファイアーウォールモジュール同士の通信を説明するシーケンス図である。

【図11】コンピュータをファイアーウォールモジュールとして動作させるためのプログラムを用いた場合の構成図である。

【図12】実施の形態2において、無線通信を使用しない場合のファイアーウォールモジュールの構成ブロック図である。

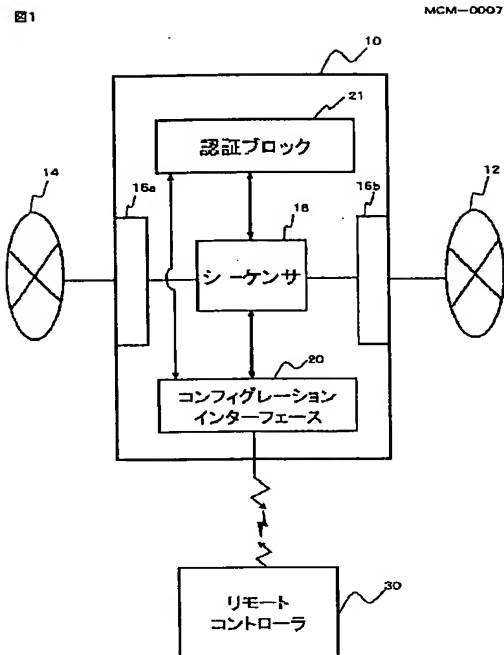
【符号の説明】

- 10 ファイアーウォールモジュール
- 10a 一方のファイアーウォールモジュール
- 10b 他方のファイアーウォールモジュール
- 12 外部ネットワーク
- 14 内部ネットワーク
- 16a インターフェース
- 16b インターフェース
- 18 シーケンサ
- 20 コンフィグレーションインターフェース
- 21 認証ブロック
- 22 メモリインターフェース
- 24a ボタンスイッチ
- 24b ボタンスイッチ
- 30 リモートコントローラ
- 32 通信手段
- 34 制御手段
- 34a ボタンスイッチ
- 34b ボタンスイッチ
- 36 メモリ手段
- 100 パケット送信
- 102 応答パケット
- 104 承認パケット
- 120 コンピュータ
- 122 ハードディスク

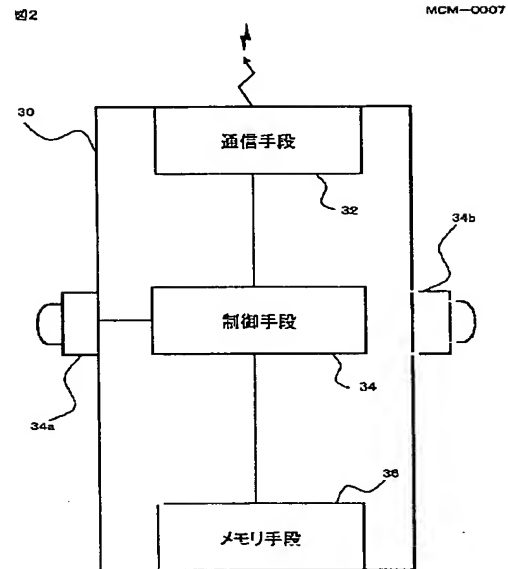
## 124 プロセッサ

## 200 インターフェース

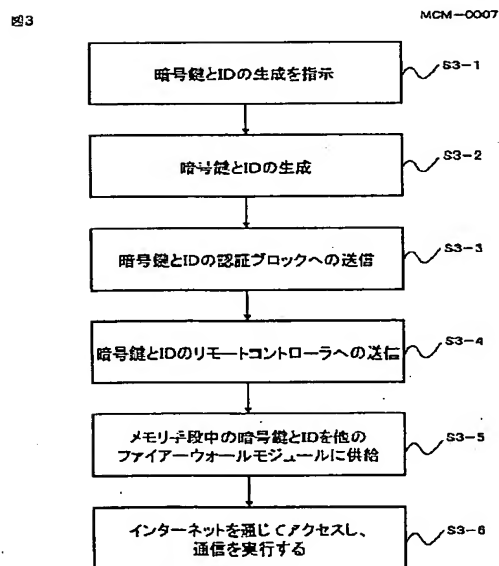
【図1】



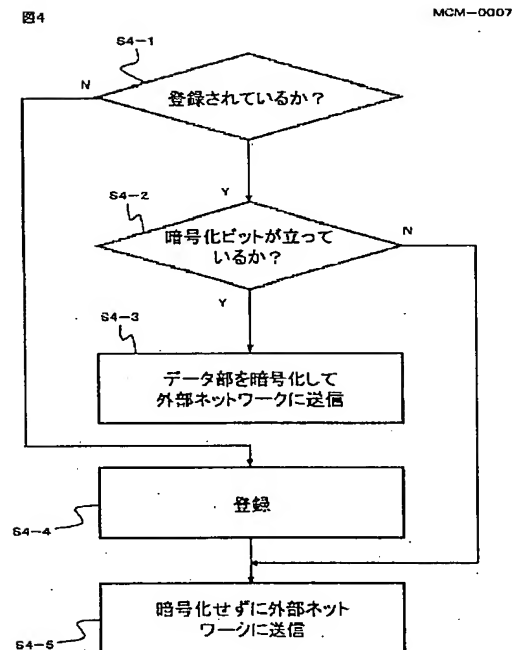
【図2】



【図3】



【図4】



【図5】

図5

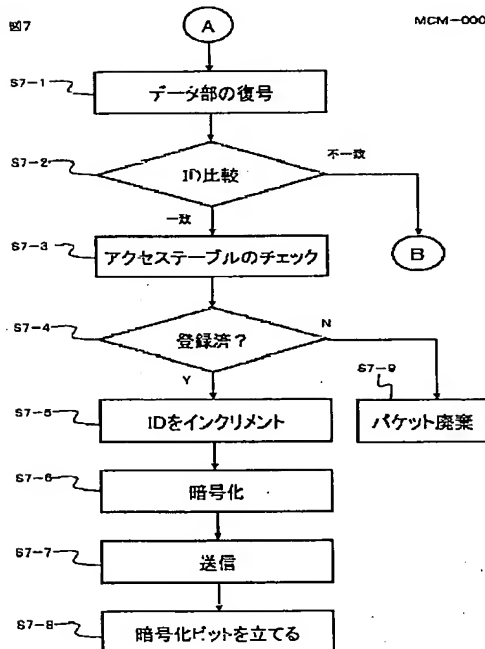
MCM-0007

パケット情報	ディスティネーション ポートナンバー	暗号化ビット
192. 168. 5. 0		0
193. 180. 7. 5		0
201. 200. 1. 128		1

【図7】

図7

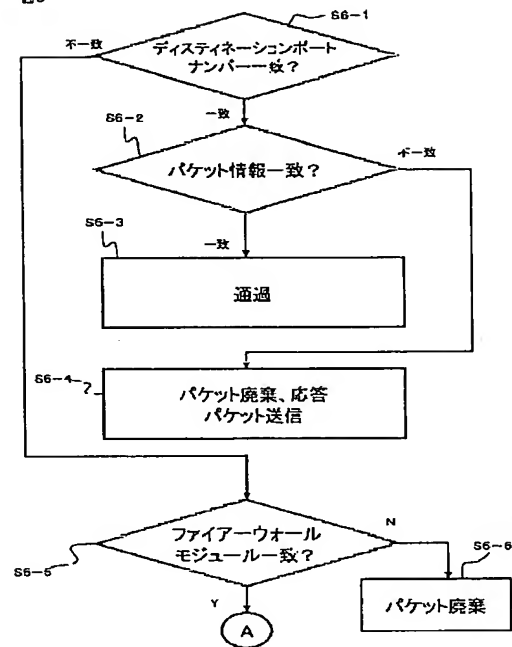
MCM-0007



【図6】

図6

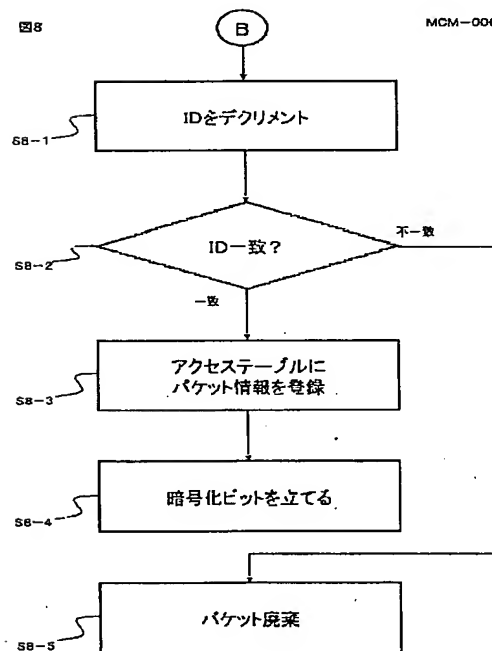
MCM-0007



【図8】

図8

MCM-0007



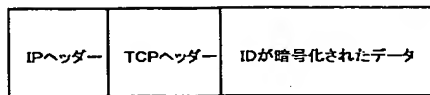


【図9】

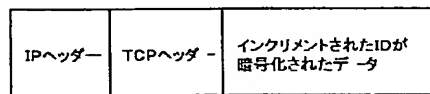
図9

MCM-0007

(1)



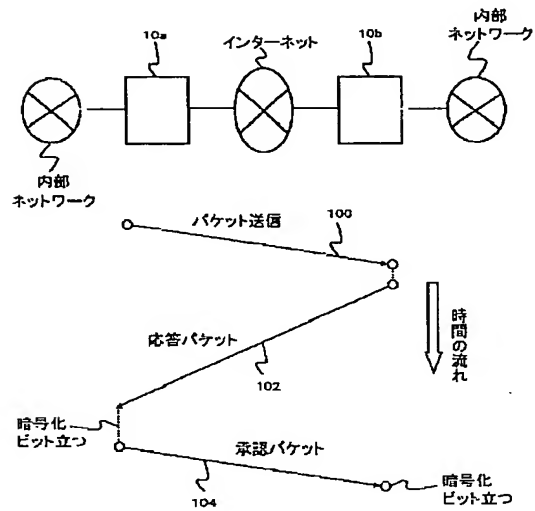
(2)



【図10】

図10

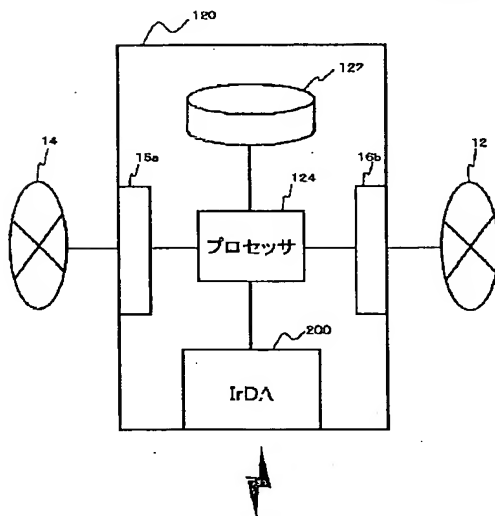
MCM-0007



【図11】

図11

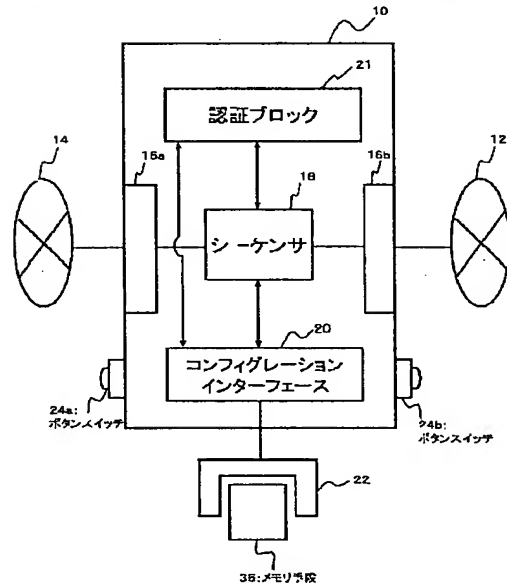
MCM-0007



【図12】

図12

MCM-0007



フロントページの続き

Fターム(参考) 5B089 GA31 GB02 JB14 KA17 KB13  
 5J104 AA16 EA04 EA22 NA02 NA41  
 5K030 GA05 GA15 HA08 HC01 HC13  
 HD03 HD06 JL01 KA04 LD19